Contribution ID: **175** Type: **Paper presentation**

Temperance Adversary Emulation Framework

Friday 19 September 2025 10:00 (15 minutes)

This paper introduces and develops Temperance, an adversary emulation framework, which can be used by the red team operators to assess the security of the target infrastructure.

To control the host during the post-exploitation phase, the operator implants an agent into the target that calls back to the C2 (Control and Command) server, from which the professionals have full remote control of the host. The network traffic that this agent generates can be distinguished from a normal user-generated one when using a standard C2 because of the beaconing behavior. The protocol used between the agent and the server influences how well the operation can scale to handle a substantial number of agents or how fast it can be stopped by the SoC (Security Operation Center).

These problems can negatively influence the capabilities of the red team to carry on the security testing. Since cybercriminals face these issues too, it's vital to find solutions before they do so that security solutions and SoC operators are ready for future cyberattacks. The solution introduced and developed by this paper uses a dynamic-size hops cluster. A hop facilitates the communication between the agents and the server in a decentralized message-passing style instead of a simple traffic forwarding, like a normal proxy.

This solution is better because some of the server's work has been delegated to the hops, requiring a lower number of active connections to be managed by it.

The infrastructure is more fault-tolerant since the cluster is increased or decreased based on the number of available hops, making the hop replacement faster and simpler. Because of this, the operators can scale the operation since human intervention is less needed to maintain the infrastructure. Some defense techniques, like IP banning, become ineffective.

To evaluate the solution, the network traffic of a normal user simulation, a baseline C2 server, and Temperance was captured to analyze the behavior. A machine learning algorithm trained to detect the beaconing behavior from the collected data was used to compare how well our solution evades this detection.

Authors: Mr BADEA, Dan Gabriel (National University of Sciences and Technology Politehnica Bucharest); Mr POCRIȘ, Sabin (National University of Sciences and Technology Politehnica Bucharest)

Presenters: Mr BADEA, Dan Gabriel (National University of Sciences and Technology Politehnica Bucharest); Mr POCRIȘ, Sabin (National University of Sciences and Technology Politehnica Bucharest)

Session Classification: Network Security

Track Classification: Networking in Education and Research